

THE CHALLENGES OF DATA SECURITY IN THE MODERN OFFICE

February 2008

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary	2
I. Background.....	3
Personal Data Transfer Devices	3
Changes in the Office Environment.....	4
II. The Impact on Data Security	6
Possible Threats	6
Information Security Trends	7
III. Planning For Data Protection	9
Awareness and Responsibility	9
Regular Assessment and Policy	9
Data Classification	10
IV. Techniques for Data Protection	11
Access Restriction.....	11
Mobile Device Protection	11
Network Protection	11
Measures To Public Channels.....	12
Appropriate Procedures.....	12
V. Conclusion	14

SUMMARY

The popular tools and technologies of modern daily life, like mobile phones, webmail, instant messaging services, removable storage media, and wireless access to the Internet, have given everyone the ability to easily carry and handle large amounts of data. Alongside this ability to carry data, many organisations have constructed information systems around products and services based on open standards and interface compatible with popular devices. In addition, organisations further facilitate easy access to data for both internal staff and the general public across the Internet, at home or in the office. But the downside to this convenience is the greater possibility of sensitive corporate data being leaked to unauthorised parties.

I. BACKGROUND

PERSONAL DATA TRANSFER DEVICES

The oldest methods of transferring computer data are through the use of removable media; physical storage devices such as tapes and disks. The latest products are tiny thumbnail-size flash drives, with data capacities going into the multiple gigabytes range that can easily store a million or more pages of text,¹ or thousands of photographs. The speed of data transfer also improves on a par with the capacity of these devices, and the common USB interface found in many devices today makes it possible to copy several tens of thousands of A4 pages of text in just a few seconds.

External storage devices come in many forms, and most of them interface with desktop computers through the popular USB interface. Examples include thumb drives, external harddisks, MP3 players, mobile phones and flash memory card readers. Some devices may even support additional wireless channels.

The latest models of mobile phone are integrated mini-computers with the same functionality as desktop computers, including a multi-media LCD screen, RAM, ROM, removable media and multi-language text input. These devices can also take photographs and record videos. Besides being a telephone, newer models are also able to communicate over wireless networking standards such as Wi-Fi (802.11 b/g) for the Internet, and Bluetooth for short-distance connection to other accessories or computers. The latest 3G protocols also enable mobile wireless connection to the Internet, including wireless web browsing and email exchange.

All these advances give ordinary people the ability to copy, store and transfer a great deal of data using relatively inexpensive devices and services.

CHANGES IN THE OFFICE ENVIRONMENT

In the old days, most corporate data systems ran on expensive mainframe or mini-computers using data archival media and networking protocols with incompatible and proprietary standards. The difficulties of interconnecting with other systems meant that access to, and the interpretation of, internal data by unrelated parties (even within the same organisation) was almost impossible since the required facilities and know-how to translate or decode data were not easily available.

System implementation costs, and the trend towards greater inter-department/organisation connections, coupled with the rise of the Internet have boosted the adoption of open standards for data systems. Applications are now developed with affordable tools available for purchase or even by free download to anybody. IT infrastructures are increasingly built on open standards that interoperate across different software and hardware platforms, and different product brands.

One of the implications is that the technical details of widely used applications and technologies, such as email systems, operating systems, and networking routers, can be studied in detail by individuals outside the organisation. This in turn means that more people have the necessary technical skills to access company information systems, and in extreme cases, uncover system weaknesses.

¹ http://www.thocp.net/reference/stones_and_pebbles/numbers.htm

Mainframe terminals have been replaced by personal computers that run on the same operating systems and interfaces used by the general public. Desktop PCs used to access critical business application data can simultaneously exchange emails through an Intranet, or out to the Internet. Data can be saved to a flash drive through a USB port in a few moments. Critical organisation data has more ways to “escape” to storage in personal devices or public messaging services, and ultimately leak out into the public domain.

II. THE IMPACT ON DATA SECURITY

POSSIBLE THREATS

Data protection used to rely on a strategy of physically shielding the raw data, that is restricting access to the bits and bytes stored in mainframes, on tapes or on disks. Such a strategy today is not effective enough in protecting data, as static shields are not applicable to modern business practices. Public clients (computers and mobile devices) are communicating with company servers using compatible interfacing standards, so anyone is able to access and interpret data from any source, provided the channels and opportunities exist. There are several ways that this could happen in the modern office, and two major channels are vulnerable: (1) Physical storage, and (2) Data networks.

1. Physical storage

Mobile devices are slim in size and convenient to carry around. They can also be lost, and if picked up by someone else, there is a possibility of information leakage. Applications in mobile phones that store contact information and calendar events may themselves contain sensitive commercial secrets. Owners disposing of an old device may forget to remove the data and content stored inside the device before disposal, and thus leave sensitive data in place for access by those with criminal intent.

A mobile device is also a potential carrier of malicious code, such as viruses and Trojan horses, that can cause an unexpected security breach if planted on a user's desktop that is connecting to the organisation network.

Mobile phones embedded with cameras are also a potential risk, in that they can be used for capturing information from hardcopy sources, or for recording video as a monitoring device.

2. Data Networks

The Internet is now a major communication channel for many businesses and organisations, and could easily become a significant data security threat. If not probably protected, organisation servers can become victims of malicious attacks from the outside, causing major damage such as loss of customer information, defacing of company websites or disruption to on-line transaction services.

Malicious code, such as viruses and Trojan horses, are an indirect way of attacking a system. They are usually spread via the Internet, embedded in downloadable files or email attachments.

Wireless LANs are now used in many office environments, but if not properly configured with data encryption turned on, wireless LAN is a potential security hole for data leakage.

Mobile phones are also now capable of accessing the Internet, but often have less security protection. Company servers and networks usually possess facilities to monitor and log connection history, but are often not able to monitor personal mobile messaging activities.

INFORMATION SECURITY TRENDS

In 2007, *InformationWeek* commissioned a Global Information Security survey conducted by consultants *Accenture*. A total of 3,092 professionals in business technology and security (1,101 U.S. respondents and 1,991 in China)² were interviewed. One of the results was a priority list of security threats which companies surveyed are most concerned about. Traditional threats relating malicious codes such as viruses are still at the top of the list. However, the following three items relating to data loss are ranked much lower;

² <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201001203>

1. *“unauthorised employee access to files and data”* is ranked number 4 by US respondents, and number 5 by Chinese respondents;
2. *“customer-data theft by outsiders”* is ranked number 5 by US respondents, and number 6 by Chinese respondents;
3. *“loss or theft of mobile devices containing corporate data”* is ranked number 7 by US respondents, and number 9 by Chinese respondents.

Despite news about data-loss incidents frequently appearing in the media, this ranking shows that the threat of data loss is still not the top priority in terms of security in many companies.

III. PLANNING FOR DATA PROTECTION

AWARENESS AND RESPONSIBILITY

Data is one of the most important assets of any organisation³, and people are usually considered to be the weakest link in the security chain⁴. It is of the utmost importance that internal staff are fully aware of their collective responsibility through education and regular reminders, so that the importance of information security is not forgotten or overlooked. Each employee must be fully aware of his or her own responsibilities, their restrictions on information access, and disciplinary action that would be taken for any breach of security. These can all serve as the driving force for self-improvement in terms of data security.

REGULAR ASSESSMENT AND POLICY

A successful project usually starts with good planning. Before making any changes, it is a good idea to assess the information systems within and across the company, and identify areas that need improvement. A security policy should be established to govern the development of subsequent guidelines and procedures. It is also important that ongoing assessments are carried out regularly so that existing procedures can be updated and refined to changes in working conditions and new technologies.

³ <http://whitepapers.zdnet.co.uk/0,1000000651,260084021p,00.htm>

⁴ http://www.schneier.com/blog/archives/2007/03/social_engineer_3.html

DATA CLASSIFICATION

Not all data may be of the same level of importance or sensitivity. For instance, information such as promotional leaflets does not need the same level of protection as say payroll data. To maximise resources, company data should be prioritised according to its security level, with security effort focused more on the most important data first.

It is also vital to assess the locations of all permanent and temporary places for storing company data, and classify their strengths in terms of data protection accordingly. For example, thumb drives are a low security storage device most suitable for less important data, while a database kept on redundant systems with backup servers that require authentication for access is more reliable for important data.

IV. TECHNIQUES FOR DATA PROTECTION

ACCESS RESTRICTION

Access to software and classified data should be restricted to authorised personnel only. Authentication with passwords and tokens are common techniques for access protection, and different authorisation profiles are often applied to different users according to their roles. Audit trails are supplementary to authentication, and comprehensive activity logs provide useful information for refining the effectiveness of security measures. Data Encryption provides another level of protection to guard against unauthorised data access.

MOBILE DEVICE PROTECTION

Mobile computing devices, along with the data inside, can easily be lost, either through theft or being left unattended. Physical protection methods, such as cable locks, are always a first line of defence. Additional authentication requirements, such as passwords, guard against unauthorised access. Users should judge the risk and necessity of storing classified information on these devices, and in any case backup their data regularly.

NETWORK PROTECTION

Protection from intrusion or attacks launched from the Internet is a big topic. A number of products including firewalls and proxy servers are already available that provide a degree of data and system protection, but it is often necessary to assess the

individual architecture of a company's data system, and design protective measures specifically to address the needs and nature of that business.

Malicious code is another form of indirect attack through a network, and again a number of advanced tools are already in place that can guard against this type of problem. The effectiveness of such guards should be maintained with regular scanning of hard disks and removable storage media, together with timely updating of patch, virus signature pattern files and malicious code definition.

MEASURES TO PUBLIC CHANNELS

Public channels of communication such as instant messaging (IM), wireless Internet access and public webmail services are possible carriers of corporate information. Measures to control their usage in the office environment are sometimes necessary:

1. Develop a clear communication usage policy and disseminate this information to all staff;
2. Consider implementing an equivalent Enterprise solution instead of using public communication services;
3. Implement gateways with security protection systems in place;
4. Disable insecure services such as the remote activation of video cameras.

APPROPRIATE PROCEDURES

During disposal of old computer equipment or media containing non-volatile data, procedures must be in place to ensure all information and data has been removed, such as physical destruction of the media itself, or by overwriting or reformatting the data stored on the media.

In some circumstances, it may be advisable to prevent staff from bringing personal belongings, including mobile phones, into the work area. This can help eliminate some of the opportunities for theft of data.

V. CONCLUSION

The IT systems used by modern offices today have migrated to open standard platforms and systems, and there are now many more channels that outsiders can take advantage of to access corporate data. The traditional technique of physically isolating the raw data alone is no longer effective in ensuring data security. Organisations must plan and review policies and procedures to protect their data. Often, a variety of measures have to be adopted, including staff education, access restrictions, audit logging, data encryption and network protection.